Next Generation Technology at a glance

(Synchronized Security vs. Best-of-Breed)

Sebastian Kaiser
Sales Engineer CEEMEA

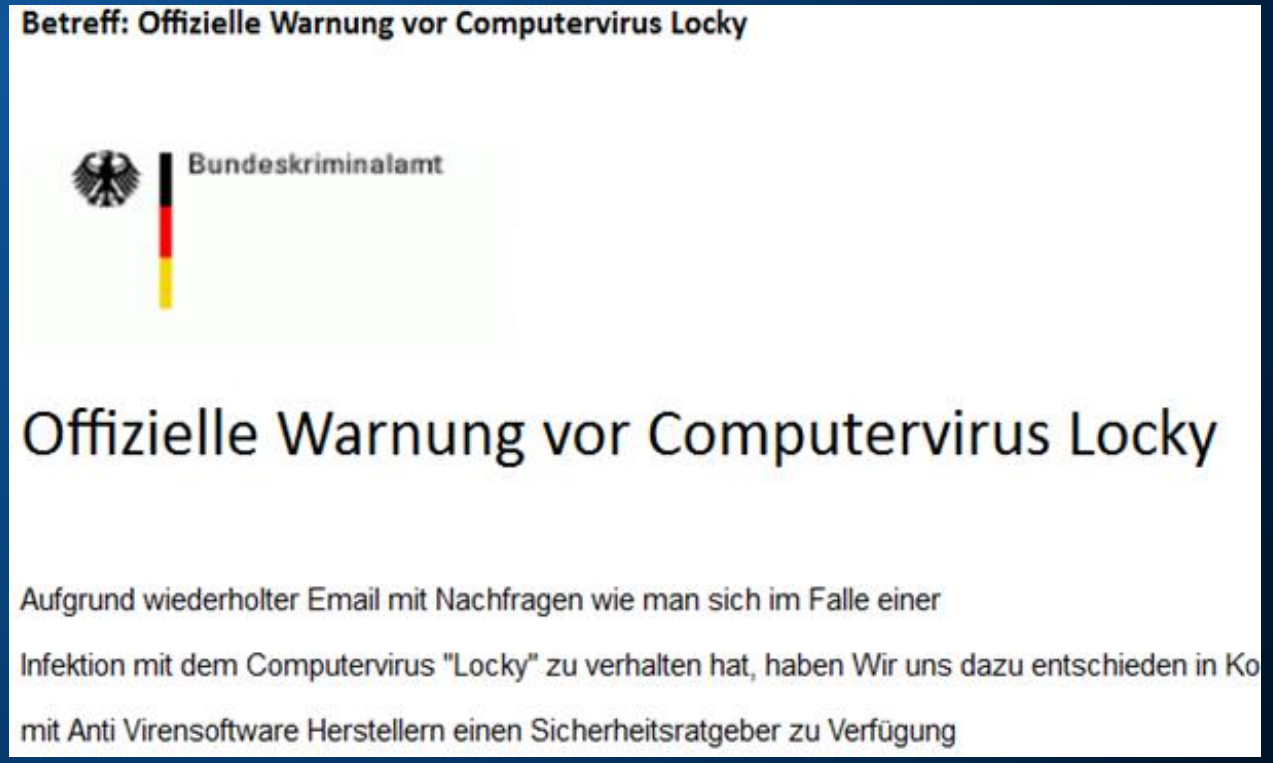
SOPHOS

Why is Ransomware so effective?

SOPHOS

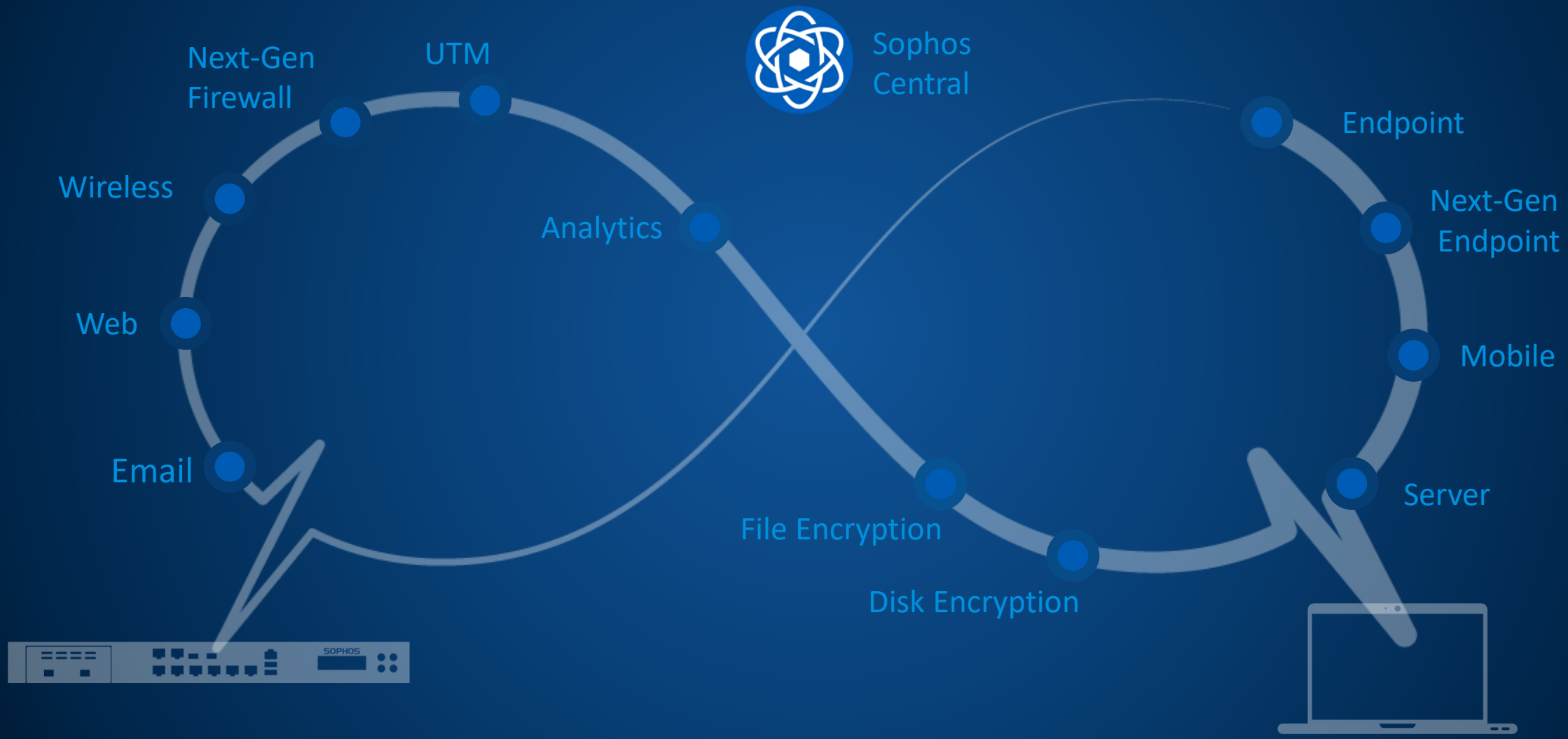
Root Cause of Infections despite Best-of-Breed Security

- Office-Documentformats and PDFs are normally allowed in E-Mail based communication
- Security Controls do not work together or act as a system
- Advanced Malware
- Professional Adversaries
- Social Engineering



Example Fantom Ransomware

Synchronized Security – Teamplay vs. Best-of-Breed

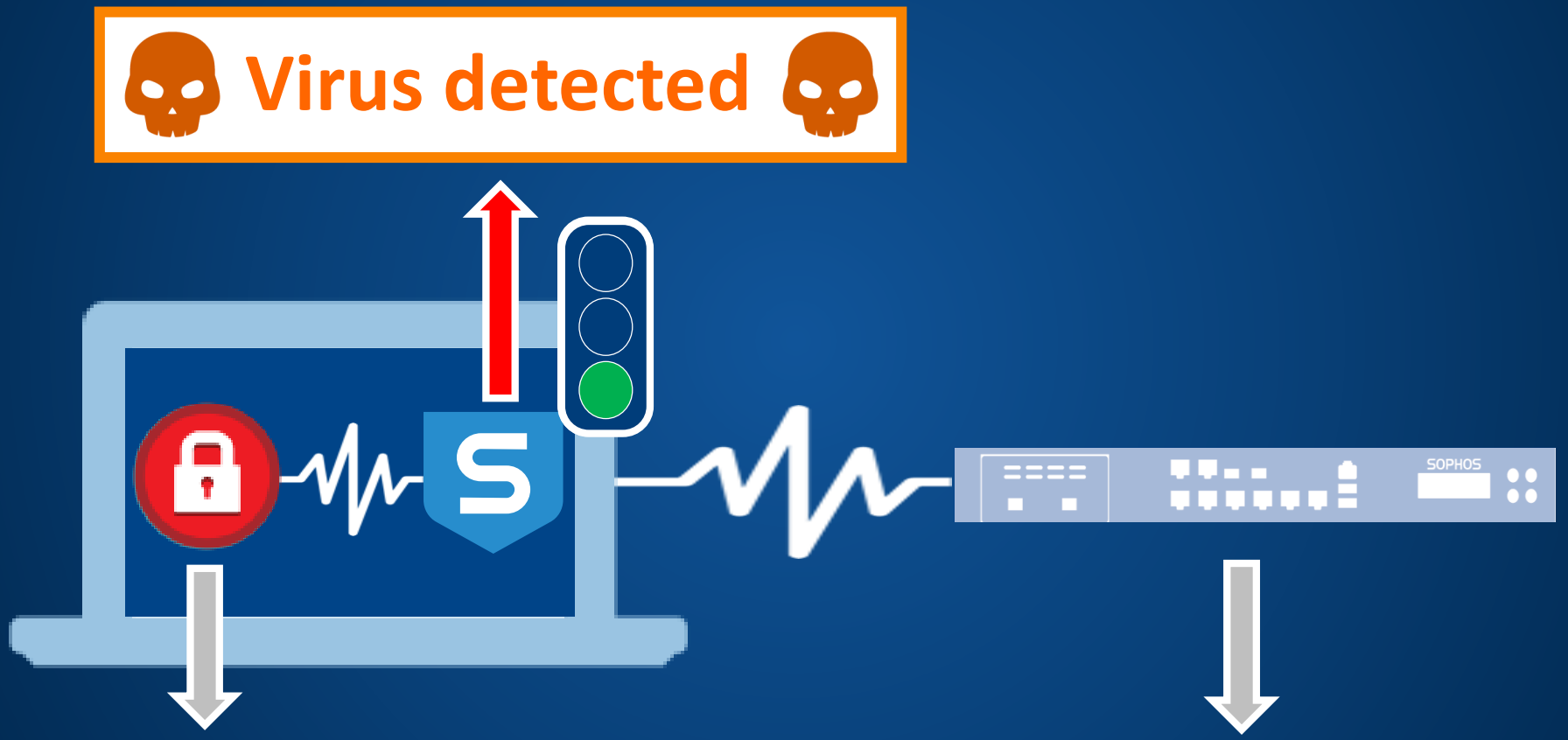


Security Heartbeat

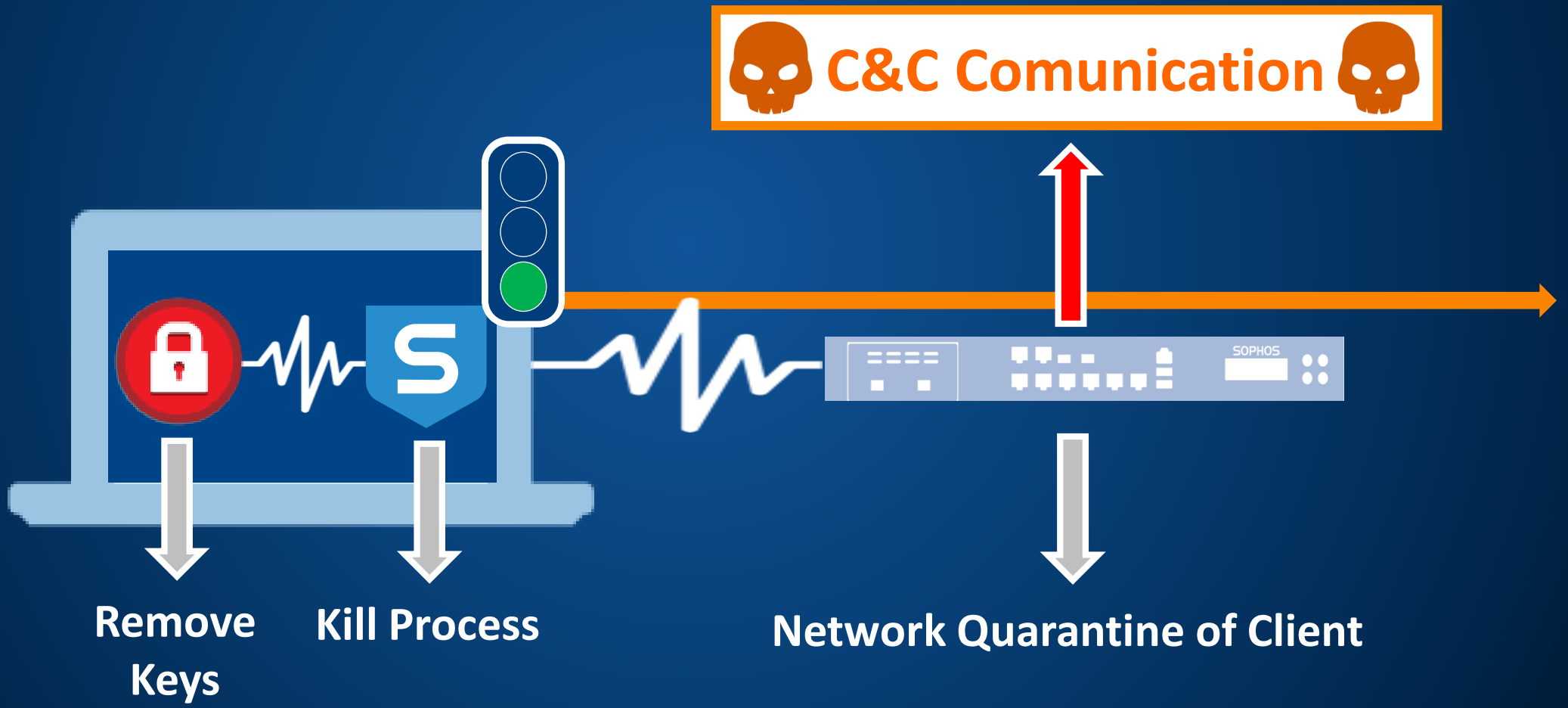
Synchronized Security

SOPHOS

Security Heartbeat – Malware Infection



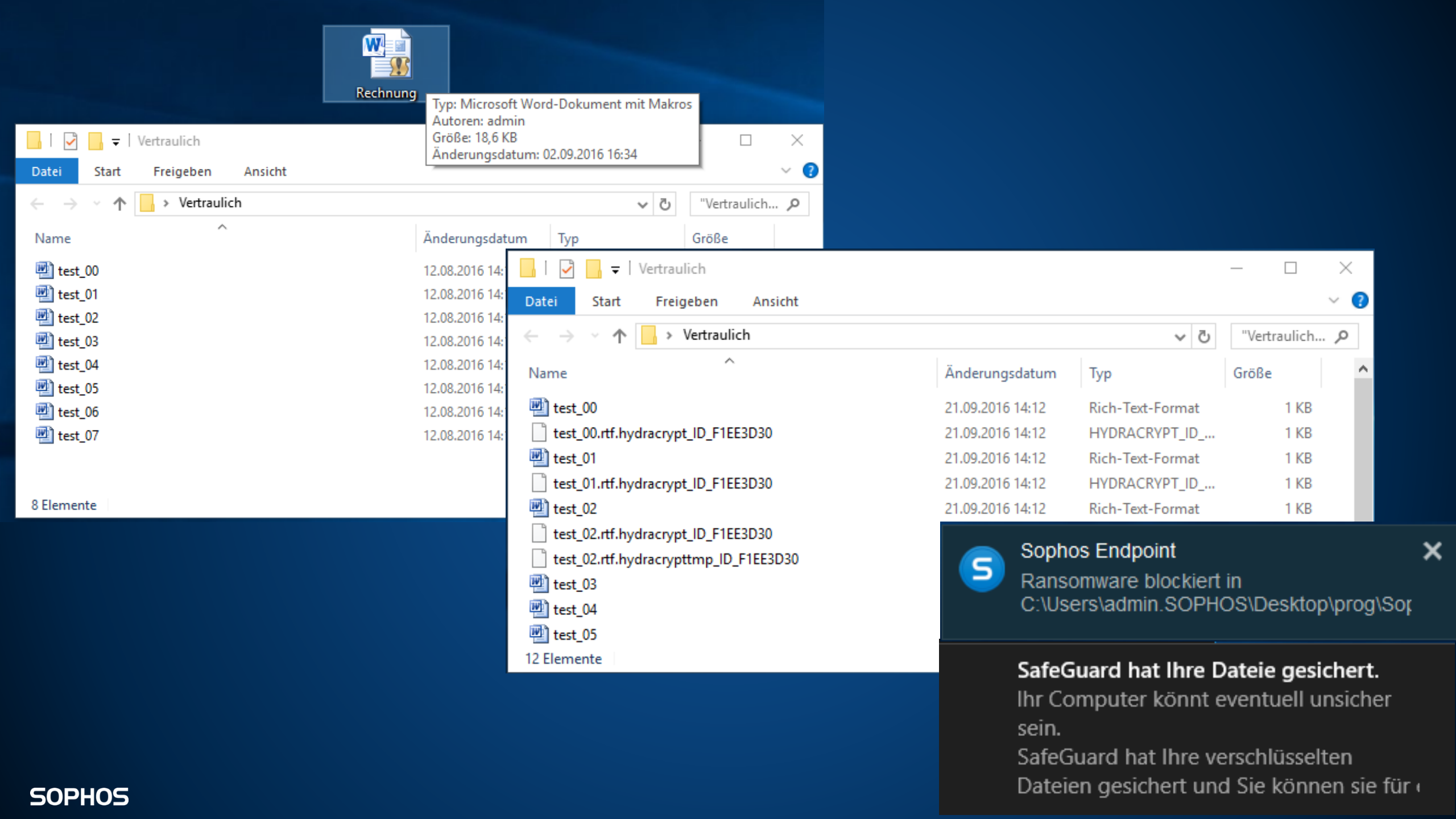
Security Heartbeat – Botnet C&C-Traffic detected

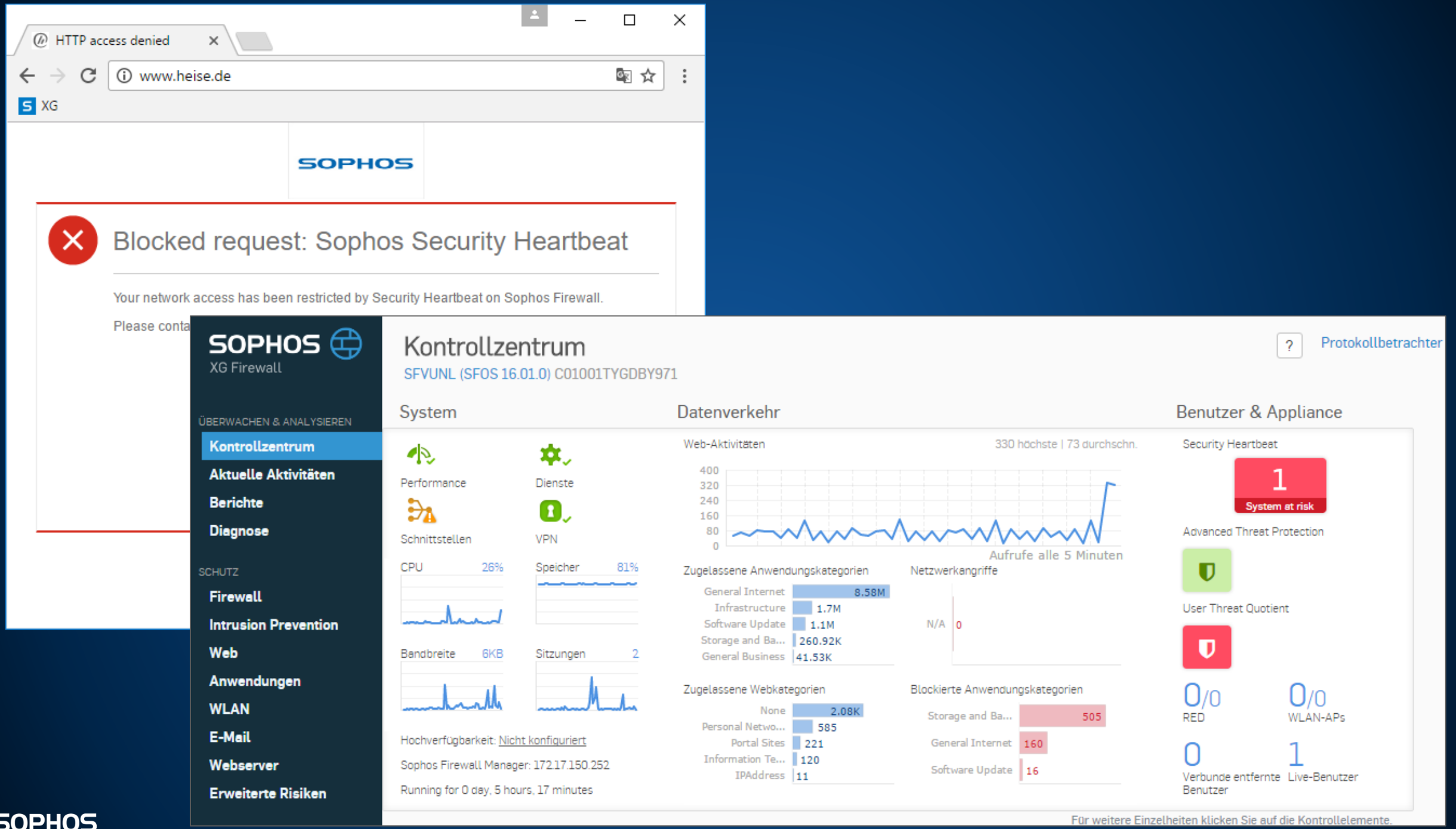


Demo

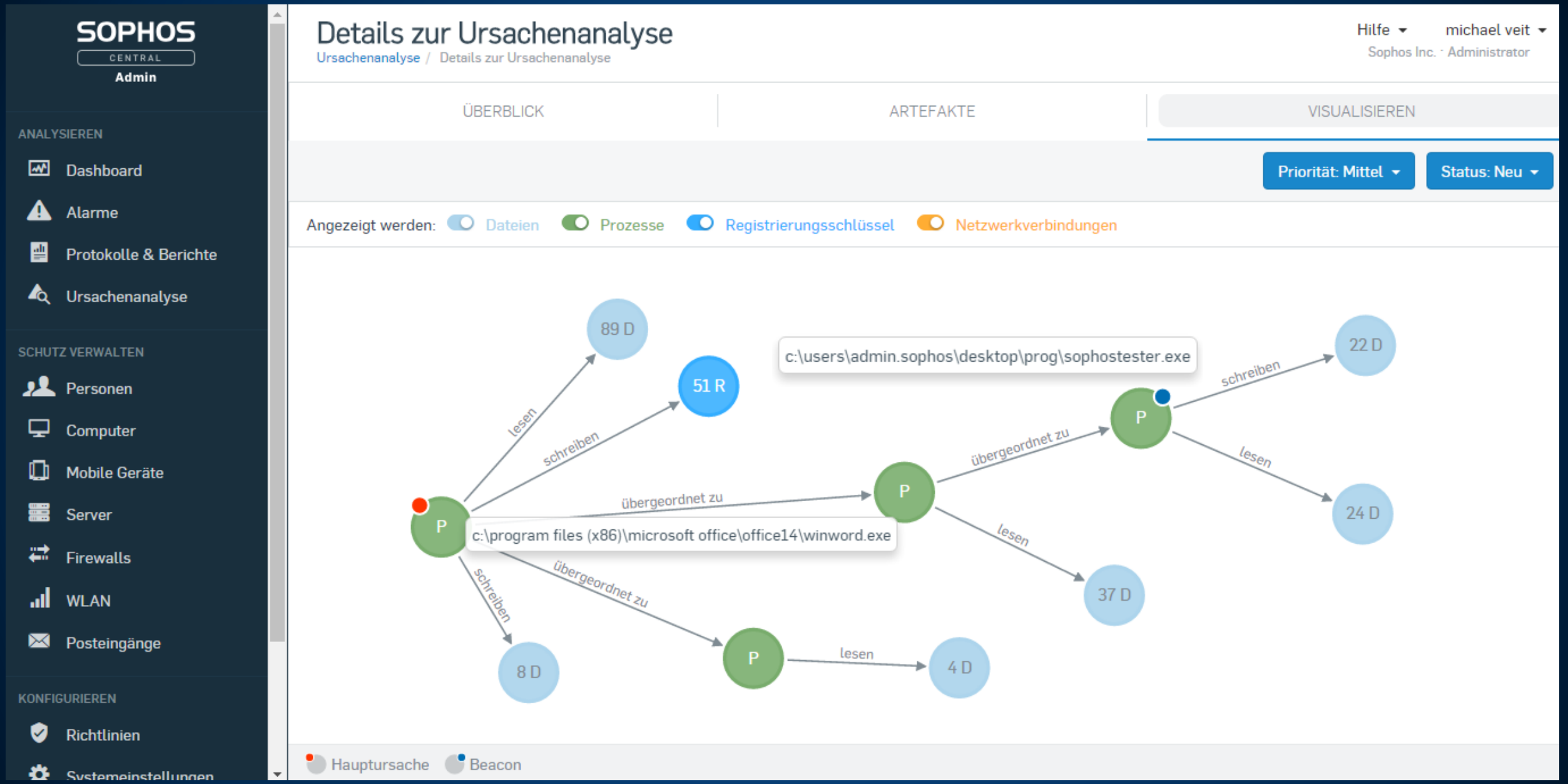
Ransomware

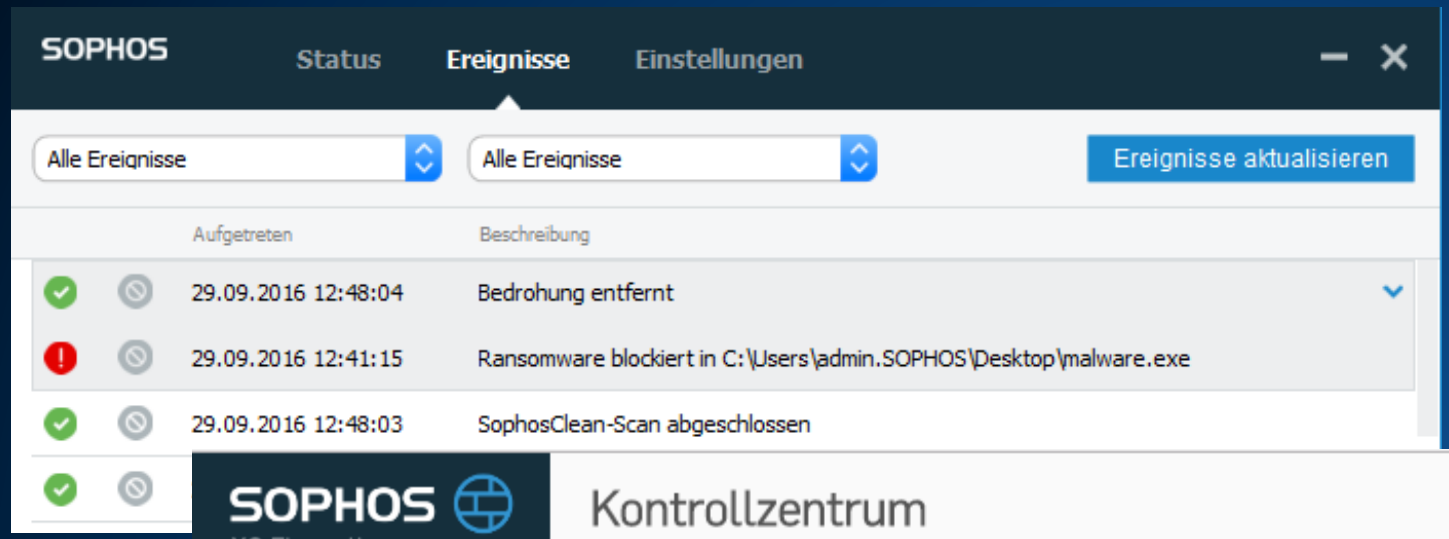
SOPHOS

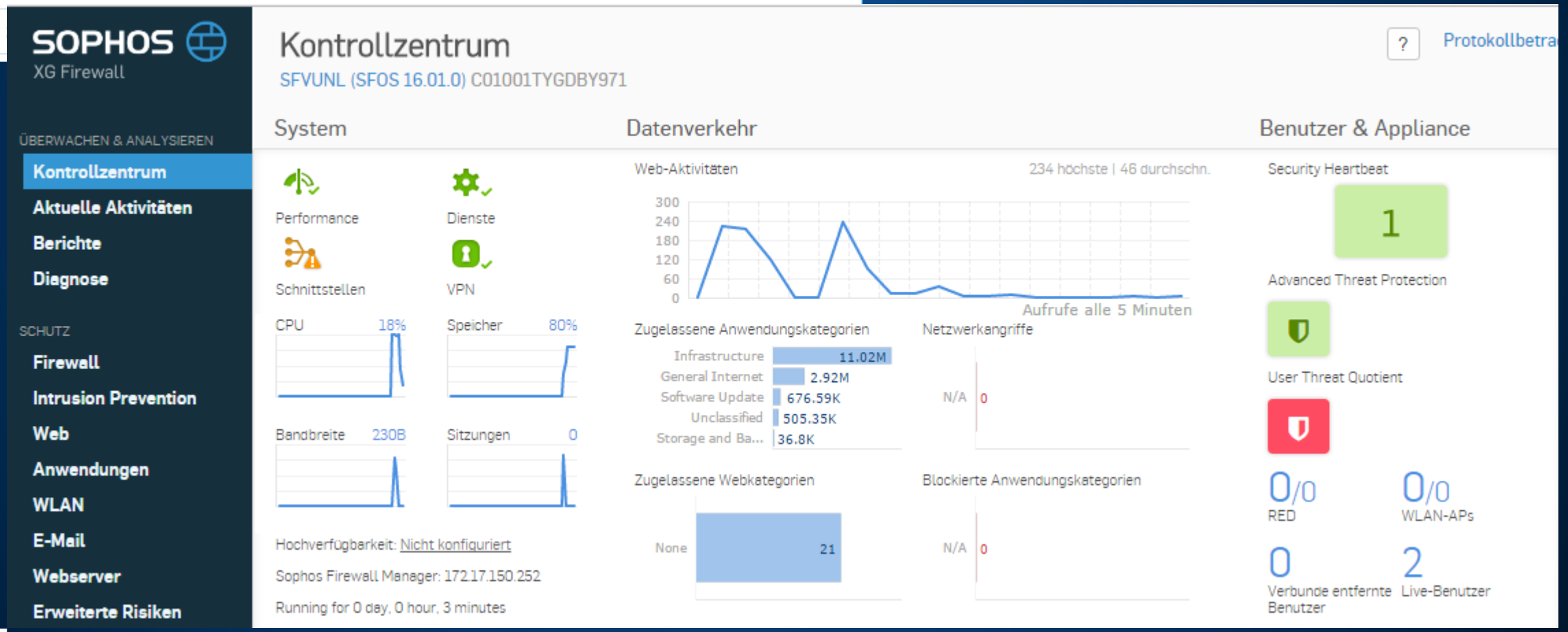

Rechnung
Typ: Microsoft Word-Dokument mit Makros
Autoren: admin
Größe: 18,6 KB
Änderungsdatum: 02.09.2016 16:34
Vertraulich
Datei
Start
Freigeben
Ansicht
Vertraulich
"Vertraulich...
Name
Änderungsdatum
Typ
Größe
test_00
test_01
test_02
test_03
test_04
test_05
test_06
test_07
12.08.2016 14:
8 Elemente
Vertraulich
Datei
Start
Freigeben
Ansicht
Vertraulich
"Vertraulich...
Name
Änderungsdatum
Typ
Größe
test_00 21.09.2016 14:12 Rich-Text-Format 1 KB
test_00.rtf.hydracrypt_ID_F1EE3D30 21.09.2016 14:12 HYDRACRYPT_ID_... 1 KB
test_01 21.09.2016 14:12 Rich-Text-Format 1 KB
test_01.rtf.hydracrypt_ID_F1EE3D30 21.09.2016 14:12 HYDRACRYPT_ID_... 1 KB
test_02 21.09.2016 14:12 Rich-Text-Format 1 KB
test_02.rtf.hydracrypt_ID_F1EE3D30
test_02.rtf.hydracrypttmp_ID_F1EE3D30
test_03
test_04
test_05
12 Elemente
Sophos Endpoint
Ransomware blockiert in
C:\Users\admin.SOPHOS\Desktop\prog\Sop
SafeGuard hat Ihre Dateie gesichert.
Ihr Computer könnt eventuell unsicher sein.
SafeGuard hat Ihre verschlüsselten Dateien gesichert und Sie können sie für
SOPHOS


HTTP access denied
www.heise.de
XG
SOPHOS
Blocked request: Sophos Security Heartbeat
Your network access has been restricted by Security Heartbeat on Sophos Firewall.
Please conta
SOPHOS
XG Firewall
ÜBERWACHEN & ANALYSIEREN
Kontrollzentrum
Aktuelle Aktivitäten
Berichte
Diagnose
SCHUTZ
Firewall
Intrusion Prevention
Web
Anwendungen
WLAN
E-Mail
Webserver
Erweiterte Risiken
Kontrollzentrum
SFVUNL (SFOS 16.01.0) C01001TYGDBY971
Protokollbetrachter
System
Performance
Dienste
Schnittstellen
VPN
CPU 26%
Speicher 81%
Bandbreite 6KB
Sitzungen 2
Hochverfügbarkeit: Nicht konfiguriert
Sophos Firewall Manager: 172.17.150.252
Running for 0 day, 5 hours, 17 minutes
Datenverkehr
Web-Aktivitäten
330 höchste | 73 durchschn.
400
320
240
160
80
0
Aufrufe alle 5 Minuten
Zugelassene Anwendungskategorien
General Internet 8.58M
Infrastructure 1.7M
Software Update 1.1M
Storage and Ba... 260.92K
General Business 41.53K
Netzwerkangriffe
N/A 0
Zugelassene Webkategorien
None 2.08K
Personal Netwo... 585
Portal Sites 221
Information Te... 120
IPAddress 11
Blockierte Anwendungskategorien
Storage and Ba... 505
General Internet 160
Software Update 16
Benutzer & Appliance
Security Heartbeat
1
System at risk
Advanced Threat Protection
User Threat Quotient
0/0
RED
0/0
WLAN-APs
0
Verbunde entfernte Benutzer
1
Live-Benutzer
Für weitere Einzelheiten klicken Sie auf die Kontrollelemente.

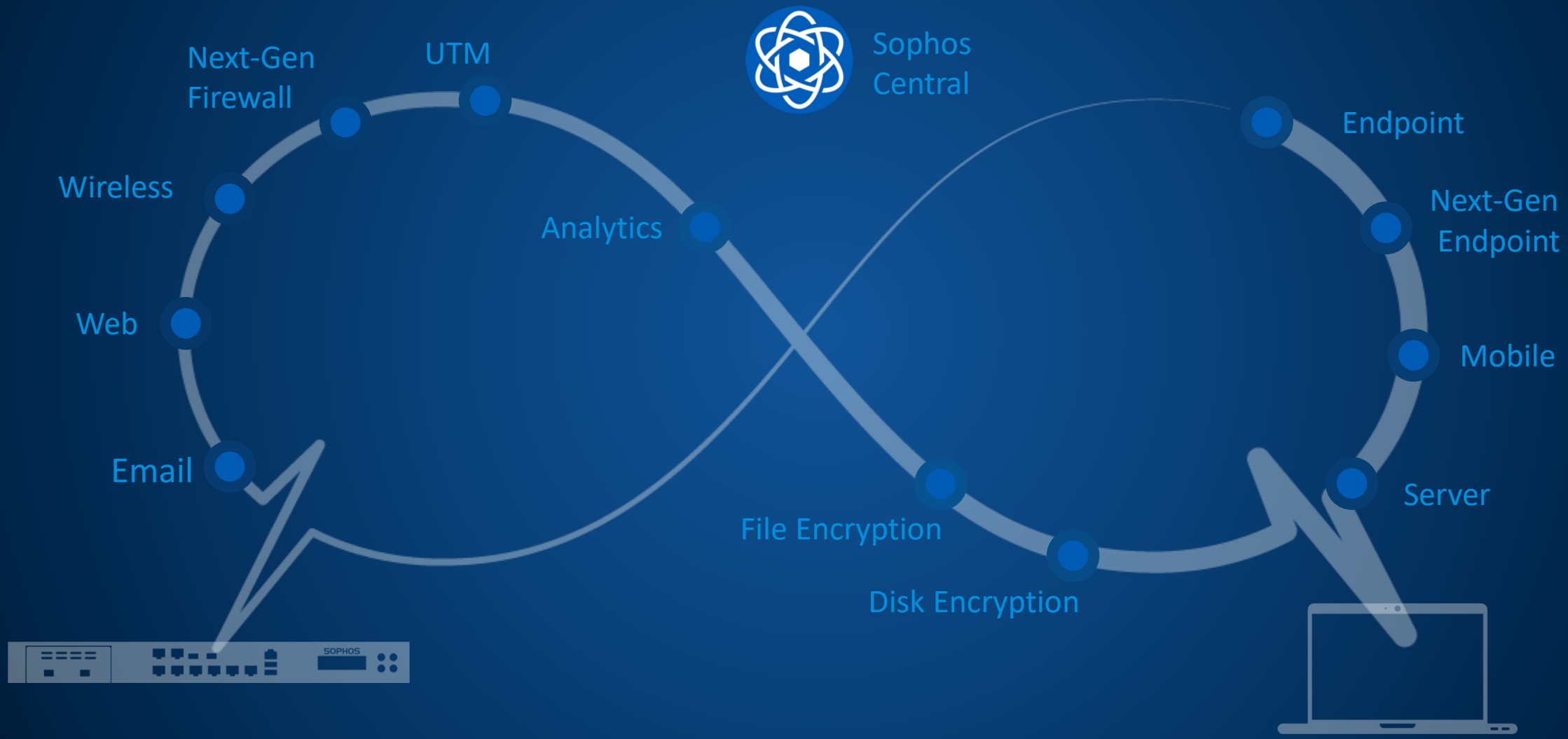
SOPHOS


SOPHOS
CENTRAL
Admin
ANALYSIEREN
Dashboard
Alarme
Protokolle & Berichte
Ursachenanalyse
SCHUTZ VERWALTEN
Personen
Computer
Mobile Geräte
Server
Firewalls
WLAN
Posteingänge
KONFIGURIEREN
Richtlinien
Systemeinstellungen
Details zur Ursachenanalyse
Ursachenanalyse / Details zur Ursachenanalyse
Hilfe
michael veit
Sophos Inc. · Administrator
ÜBERBLICK
ARTEFAKTE
VISUALISIEREN
Priorität: Mittel
Status: Neu
Angezeigt werden:
Dateien
Prozesse
Registrierungsschlüssel
Netzwerkverbindungen
89 D
51 R
lesen
schreiben
c:\users\admin.sophos\desktop\prog\sophostester.exe
22 D
schreiben
P
übergeordnet zu
lesen
24 D
P
übergeordnet zu
c:\program files (x86)\microsoft office\office14\winword.exe
lesen
37 D
P
schreiben
übergeordnet zu
8 D
P
lesen
4 D
Hauptursache
Beacon


SOPHOS
Status
Ereignisse
Einstellungen
Alle Ereignisse
Alle Ereignisse
Ereignisse aktualisieren
Aufgetreten
Beschreibung
29.09.2016 12:48:04
Bedrohung entfernt
29.09.2016 12:41:15
Ransomware blockiert in C:\Users\admin.SOPHOS\Desktop\malware.exe
29.09.2016 12:48:03
SophosClean-Scan abgeschlossen


SOPHOS
XG Firewall
Kontrollzentrum
SFVUNL (SFOS 16.01.0) C01001TYGDBY971
Protokollbetra
ÜBERWACHEN & ANALYSIEREN
Kontrollzentrum
Aktuelle Aktivitäten
Berichte
Diagnose
SCHUTZ
Firewall
Intrusion Prevention
Web
Anwendungen
WLAN
E-Mail
Webserver
Erweiterte Risiken
System
Performance
Dienste
Schnittstellen
VPN
CPU 18%
Speicher 80%
Bandbreite 230B
Sitzungen 0
Hochverfügbarkeit: Nicht konfiguriert
Sophos Firewall Manager: 172.17.150.252
Running for 0 day, 0 hour, 3 minutes
Datenverkehr
Web-Aktivitäten
234 höchste | 46 durchschn.
300
240
180
120
60
0
Aufrufe alle 5 Minuten
Zugelassene Anwendungskategorien
Infrastructure 11.02M
General Internet 2.92M
Software Update 676.59K
Unclassified 505.35K
Storage and Ba... 36.8K
Netzwerkangriffe
N/A 0
Zugelassene Webkategorien
None 21
Blockierte Anwendungskategorien
N/A 0
Benutzer & Appliance
Security Heartbeat
1
Advanced Threat Protection
User Threat Quotient
0/0
RED
0/0
WLAN-APs
0
Verbunde entfernte Benutzer
2
Live-Benutzer

Synchronized Security – Teamplay vs. Best-of-Breed



Synchronized Security by Sophos

- Best-of-Breed will be replaced by Security as a System
- Intercommunication of Network-, Endpoint- and Encryption Controls are mandatory
- Detection of Advanced Threats (e.g. Exploit techniques)
- Identification of compromised assets in realtime
- Automation of Incident Response and Remediation
- Security Analytics (attack path, trajectories and lateral movement)

SOPHOS

Security made simple.